In the Claims:

1. (Previously Presented) A method for secure distribution of digital content to an untrusted environment of an intended recipient of said digital content, comprising the steps of:

gathering information about said digital content's intended recipient environment;

producing trustworthiness credentials about said intended recipient environment based on said information;

selecting protective measures for distributing said digital content in accordance with said trustworthiness credentials;

distributing digital content secured by said selected protective measures to said untrusted environment;

constructing a trusted environment within said untrusted environment;

constructing from said digital content at least two digital input sources, said digital input sources being operable in combination in order to produce a screen rendered version of said digital content;

transferring said digital content to said trusted environment such that each of said input sources is transmitted via a different path; and

combining said input sources within said trusted environment in order to produce said screen rendered version of digital content, said trusted environment otherwise preventing access to said digital input sources.

2. (Original) A method according to claim 1 wherein said digital content is a document.

3. (Previously Presented) A method according to claim 1 wherein said digital content is multimedia digital content.

4 - 5. (Canceled)

6. (Original) A method according to claim 3 wherein said multimedia digital content consists of at least two different streams.

7 - 10. (Canceled)

11. (Previously Presented) A method according to claim 1 wherein said trusted environment comprises a software component.

12 - 14. (Canceled)

15. (Previously Presented) A method according to claim 1 wherein said trusted environment comprises a hardware component.

16. (Canceled)

17. (Previously Presented) A method according to claim 1 wherein said trusted environment comprises a firmware component.

18 - 20. (Canceled)

21. (Previously Presented) A method according to claim 1 wherein said trusted environment comprises at least two components.

22. (Original) A method according to claim 21 wherein at least one of said components comprises a software component.

23 - 34. (Canceled)

35. (Previously Presented) A method according to claim 1 wherein at least one of said input sources comprises a scrambled copy of said digital content, and at least one other input source comprises the information needed for said reproduction.

36. (Previously Presented) A method according to claim 1 wherein a group of at least two of said input sources comprises a function of a scrambled copy of said digital content, and at least one other input source comprises the information needed for reconstruction.

37 - 58. (Canceled)

59. (Previously Presented) A method according to claim 1 wherein said digital content is split into said separate input sources in a trusted server, said server is operable to deliver said digital content to said trusted environment in the form of said separate input sources.

60 - 70. (Canceled)

71. (Previously Presented) A method according to claim 1 wherein said credentials comprise information gathered in the past.

72 - 73. (Canceled)

74. (Previously Presented) A method according to claim 1 wherein said credentials comprise information about the environment into which said digital content is to be distributed.

75 - 79. (Canceled)

80. (Previously Presented) A method according to claim 1 wherein said credentials comprise reports from at least one trusted component.

81 - 179. (Canceled)

180. (Previously Presented) A method according to claim 1 wherein said credentials comprise geo-location information.

181. (Previously Presented) A method according to claim 1 wherein said credentials comprise geo-location authentication level information.